(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 215 907 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
19.06.2002 Bulletin 2002/25

(51) Int Cl.[7]: **H04N 7/24**

(21) Application number: **01310112.6**

(22) Date of filing: **03.12.2001**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **07.12.2000 GB 0029851**
31.08.2001 GB 0121202

(71) Applicant: **SONY UNITED KINGDOM LIMITED**
Weybridge KT13 0XW (GB)

(72) Inventors:
- **Stone, Jonathan James**
  Berkshire RG7 3SS (GB)
- **Pelly, Jason Charles**
  Berkshire RG6 4DU (GB)
- **Gugenheim, Paul**
  London NW6 1XN (GB)
- **Delacour, Isabel**
  Hampshire RG22 4BB (GB)
- **Foster, Richard**
  Hampshire SP6 3LF (GB)

(74) Representative: **Pratt, Richard Wilson et al**
D. Young & Co,
21 New Fetter Lane
London EC4A 1DA (GB)

(54) Watermarking material and transferring watermarked material

(57) A system for watermarking and transferring watermarked material comprises a transaction server, first and second clients, first apparatus for applying a perceptible watermark to the material and second apparatus for removing the watermark. The server, clients and first and second apparatus are linked by one or more communications networks. The system is arranged to implement the steps of:

transferring from the transaction server to the first apparatus (i) data for creating a watermark, the creating data including (a) data defining an invertible algorithm and (b) data for creating at least one security key associated with the algorithm and (ii) data for creating a material identifier;
using the said first apparatus to apply a material identifier to the material and applying a watermark to the material, using the said creating data;
transferring from the first client to the transaction server the said material identifier and data for inverting the algorithm including the said at least one key;
transferring the watermarked material to the second apparatus;
deriving the said material identifier from the material;
transferring the identifier from the second client to the transaction server;
subject to predetermined conditions being satisfied, transferring from the transaction server to the second apparatus watermark removal data associated with the said material identifier, the removal data including at least one key and data defining an algorithm for removing the watermark in conjunction with the key; and
using the second apparatus to remove the watermark using the said removal data.

EP 1 215 907 A2

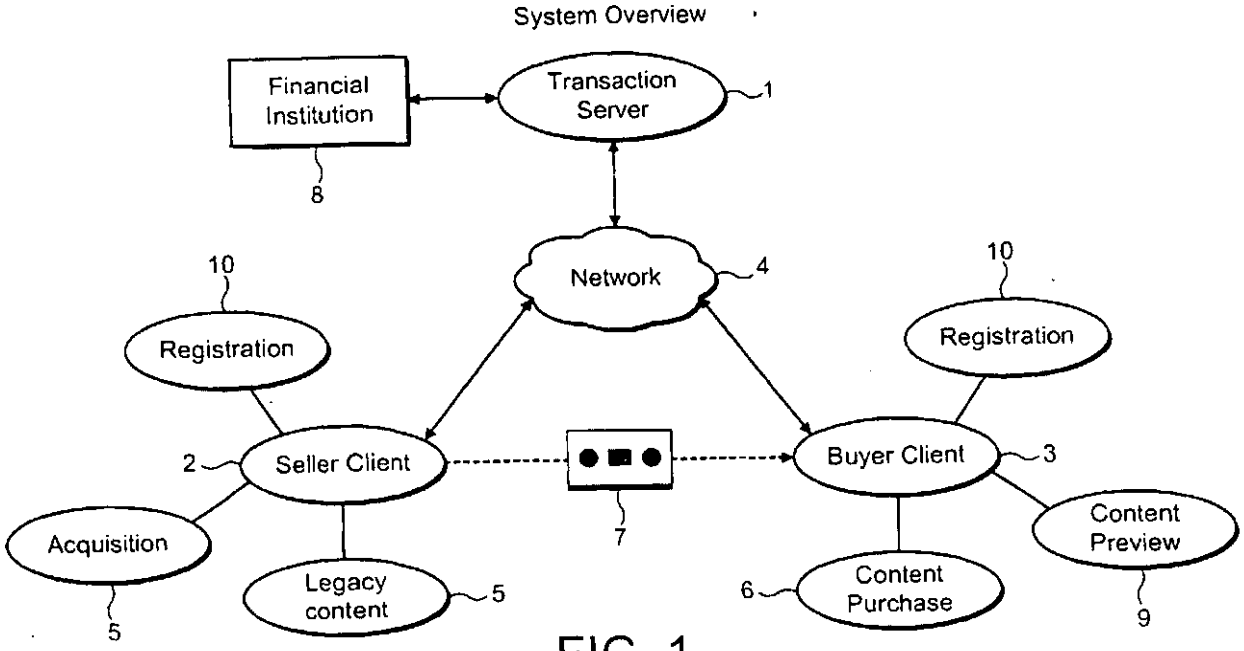

System Overview
Financial Institution
8
Transaction Server
1
Network
4
10
Registration
2
Seller Client
Acquisition
5
Legacy content
5
7
10
Registration
Buyer Client
3
Content Preview
9
6
Content Purchase

FIG. 1

Description

[0001] The present invention relates to watermarking material and to transferring watermarked material.

[0002] Material means one or more of image material, audio material and data material. Image material is generic to still and moving images and includes video, whether compressed or not.

[0003] This specification uses the terms "seller" and "buyer" in relation to such material for convenience and ease of description.. It will be appreciated that those terms do not simply mean someone (seller) who transfers outright ownership to someone else (buyer) for a consideration usually money. Often, material is licensed to a user (buyer) by a licensor (seller) who allows the licensee to use the material in accordance with defined terms or business rules. Thus the terms seller and buyer have more general meanings and include intermediaries acting on behalf of other persons who may be the ultimate owners of the material and the ultimate users thereof.

[0004] It is known to watermark material. Data may be embedded as a watermark in the material. A watermark may be imperceptible or perceptible in the material. The present invention uses perceptible watermarks and optionally may also use imperceptible watermarks.

[0005] A watermark may be used for various purposes. It is known to use watermarks for the purpose of protecting the material against, or trace, infringement of the intellectual property rights of the owner(s) of the material. For example a watermark may identify the owner of the material.

[0006] Watermarks may be "robust" in that they are difficult to remove from the material. Robust watermarks are useful to trace the provenance of material which is processed in some way either in an attempt to remove the mark or to effect legitimate processing such as video editing or compression for storage and/or transmission. The present invention uses robust watermarks. Watermarks may be "fragile" in that they are easily damaged by processing which is useful to detect attempts to remove the mark or process the material.

[0007] It is known to offer watermarked images for sale over the internet. Watermarked images may be downloaded for inspection and for examination for suitability for the users' desired purpose. If the user wishes to purchase an unwatermarked image, the user agrees to conditions of sale, for example an end user License, and pays for the image e.g. by credit card. The user is then able to download the unwatermarked image. See for example http://www.eyewire.com/help/.

[0008] It is desirable to provide a system in which one user (e.g. a seller) is provided with a system for watermarking material and another user (e.g. a buyer) is provided with a secure method and system for removing the watermark, together with a secure system for transferring watermarked material between sellers and buyers.

[0009] According to one aspect of the present invention, there is provided a method of watermarking and transferring watermarked material in a system comprising a transaction server, first and second clients, first apparatus for applying a perceptible watermark to the material and second apparatus for removing the watermark; the method comprising the steps of:

transferring from the transaction server to the first apparatus (i) data for creating a watermark, the creating data including (a) data defining an invertible algorithm and (b) data for creating at least one security key associated with the algorithm and (ii) data for creating a material identifier;

using the said first apparatus to apply a material identifier to the material and applying a watermark to the material, using the said creating data;

i transferring from the first client to the transaction server the said material identifier and data for inverting the algorithm including the said at least one key;

transferring the watermarked material to the second apparatus;

deriving the said material identifier from the material;

transferring the identifier from the second client to the transaction server;

subject to predetermined conditions being satisfied, transferring from the transaction server to the second apparatus watermark removal data associated with the said material identifier, the removal data including at least one key and data defining an algorithm for removing the watermark in conjunction with the key; and

using the second apparatus to remove the watermark using the said removal data.

[0010] The method allows originators or owners of material to offer it for sale to buyers in a secure manner. The transaction processor allows many sellers to offer material for sale and for many buyers to buy. The transaction processor allows sellers, who have access to a first client and access to a watermarking apparatus to design and apply secure watermarks without needing to know how, in detail, the watermarking is achieved. Thus apart from knowing how to co-operate with the server, the sellers do not require skills special to watermarking. Likewise buyers who have access to a second client and a watermark removal apparatus do not need such special skills to remove watermarks once they have complied with the said predetermined conditions.

[0011] The security key provides security against unauthorised removal of the watermark. The data for inverting the algorithm including the said at least one key is transferred to the transaction processor, without such data being on or with the material thereby providing further security.

[0012] In a preferred embodiment, the data for apply-

ing the algorithm including the said at least one key is stored in data carrier, most preferably a smart card. The smart card co-operates with the first apparatus during compression to apply the watermark. The smart card is used to securely transfer the data for inverting the algorithm including the said at least one key from the first apparatus to the first client for transfer to the transaction server.

[0013] The said watermark creating data may be stored on data carrier, most preferably a smart card, in response to a request for the data sent from the first client to the transaction processor. In one embodiment the said data is transferred from the transaction server to the first client and then to the smart card. In another embodiment the smart card, with the creation data stored thereon, may be sent to the operator of the first apparatus by e.g. post.

[0014] The said watermark removal data may likewise be transferred from the transaction server to the second apparatus in a data carrier, most preferably a smart card.

[0015] In one embodiment the said data is transferred from the transaction server to the second client and then to the smart card. In another embodiment, a request for the said data is received by the transaction processor and the said data is stored on the smart card and the card is sent to the operator of the second apparatus, e. g. by post.

[0016] The watermarked material may be transferred from the first apparatus to the second on a recording medium, for example a disc or tape, by for example post. Alternatively, the watermarked material may be transferred via an electronic communications network, possibly in compressed format.

[0017] Another aspect of the invention provides a method of watermarking and transferring watermarked material in a system comprising a transaction server and at least first and second clients, the method comprising the steps of:

Using the first client to (i) create a watermark, defined by (a) an invertible algorithm and (b) at least one security key associated with the algorithm and (ii) provide a material identifier;
using the said first client to associate the material identifier with the material and apply the watermark to the material;
and storing, in the transaction server, the said material identifier and data for inverting the algorithm including the said at least one key;
transferring the watermarked material to the second client;
deriving the said material identifier associated with the material;
transferring the identifier from the second client to the transaction server;
subject to predetermined conditions being satisfied, transferring from the transaction server to the second client watermark removal data associated with the said material identifier, the removal data including at least one key and data defining an algorithm for removing the watermark in conjunction with the key; and
using the second client to remove the watermark using the said removal data. In an embodiment the watermark is created by interaction of the first client with the server.

[0018] Other aspects of the invention are specified in the claims to which attention is invited.

For a better understanding of the present invention, reference will now be made by way of example to the accompanying drawings in which:

Figure 1 is a schematic diagram of a material transfer system in accordance with a first example embodiment of the invention;
Figure 2 is a schematic diagram illustrating seller registration;
Figure 3 is a schematic diagram of an example of a smart card;
Figure 4 is a schematic diagram of another example of a smart card;
Figure 5 is schematic diagram illustrating material acquisition;
Figure 6 is a schematic diagram illustrating the application of the invention to legacy material;
Figure 7 is a schematic diagram of a tape on which a material identifier and watermarked material is recorded;
Figures 8 and 9 illustrate transaction server functions;
Figure 10 is schematic diagram illustrating material purchase;
Figure 11 a schematic diagram of a material transfer system in accordance with a second example embodiment of the invention;
Figure 12 is a schematic diagram illustrating seller registration in a second example embodiment of the invention;
Figure 13 is a schematic diagram illustrating buyer registration in the second example embodiment of the invention; and
Figures 14 and 15 schematically illustrate files stored in a transaction processor of the system of Figure 11.

First Example- Figures 1 to 10

Overview, Figure 1.

[0019] Referring to Figure 1, a first example of a system in accordance with the invention comprises a transaction server, a seller client 2, a buyer client 3 and a communications network 4 linking the clients to the server.

[0020] The owner of material, i.e. the seller, controls the seller client 2. A buyer controls the buyer client 3. A third party owns and controls the transaction processor 1. The system allows material to be acquired, securely and visibly watermarked, and transferred to the buyer for the buyer to preview (9) the watermarked material. If the buyer then wants to buy the material, the buyer obtains from the transaction server 1 the data needed to remove the watermark. In this example, the seller and buyer both register (10) with the transaction server. Registration, content preview, and watermark removal are described in more detail hereinbelow. The data for removal of the watermark is sent to the buyer only when the buyer has paid for the material. The payment is monitored by the transaction server I which communicates with a financial institution 8. Payment is made via the server 1 and/or via the institution 8.

[0021] Associated with the seller client 2 is a first apparatus 5 for compressing video material and for applying a watermark to the material as part of the compression process. An example of such apparatus and process are disclosed in copending British application 0029850.5, attorney fileP/10145,I-00-147 the content of which is incorporated herein by virtue of this reference to it. Figure 1 denotes such apparatus at 5 by "legacy" and "acquisition" which will be described in more detail below in the sections "legacy" and "acquisition". Associated with the buyer client 3 is a second apparatus 6 for removing the watermark. An example of such apparatus and process are disclosed in copending application 0029850.5, attorney fileP/10145, I-00-147 the content of which is incorporated herein by virtue of this reference to it. Figure 1 denotes such apparatus at 6 by "content purchase" which will be described in more detail below in the section "content purchase".

[0022] In this example the material is video material and is recorded on a tape 7 which will be described in more detail with respect to Figure 7. The material is acquired and watermarked by the first apparatus 5. In addition a material identifier is applied to the material. Then the material is transferred on the tape to the second apparatus 6. The transfer is for example by post.

[0023] An identifier is applied to the material. An example of an identifier is a Unique Material Identifier or UMID. UMIDs are described in more detail in SMPTE Journal March 2000.

Seller Registration, Figure 2.

[0024] The seller client 2 is used to send to the transaction server 1 a) passwords, b) bank account details of the seller and c) any other information. The transaction server may then send a data carrier, in this example a smart card SC, to the seller. The seller inserts the smart card into the client 2 and communicates with the server 1. The seller designs the form of the watermark to be applied to the material using the server. The form of the watermark is defined by a bit map, also referred to herein as the template. The seller also obtains from the server an algorithm for creating the watermark including one or more security key generators for applying the watermark and a UMID generator. The seller may choose an algorithm from several available in the server. The template, algorithm, key generators and UMID generator are downloaded onto the smart card for transfer to the seller.

Smart Card, Figures 3 and 4.

[0025] Smart cards are well known. A smart card may have a processor and memory as shown in Figure 3, or may have memory but no processor as shown in Figure 4.

[0026] In the example of Figure 3, the card SC has a processor SC1, a template store SC2, a key generator SC3, a UMID generator SC4 and a store SC5. The template store SC2 stores the template defining the form of the watermark. The processor is programmed to implement the algorithm. The processor SC1 receives a representation of the image to be watermarked and uses the keys generated by the generator SC3 and the template to apply the watermark. Keys generated by the generator SC3 are stored in the store SC5. Each piece of material is assigned a UMID. Each UMID is also stored in store SC5 in association with the keys generated for that piece of material. The representation of the image may be a spatial domain image or a transform of the image used for compression of the image.

[0027] In preferred embodiments, the smart card of Figure 3 cooperates with an external processor which for example produces transform coefficients as part of a compression process and the processor SC1 applies the watermarking algorithm to the coefficents.

[0028] In the example of Figure 4, the smart card contains only memories SC5', SC2' and SC6. SC5' is a UMID and key store, SC2' is a template store and SC6 stores algorithm configuration data. The card of Figure 4 operates in conjunction with an external processor to apply a watermark to material. UMIDs and keys generated in that process are stored in the store SC5'.

Acquisition, Figure 5.

[0029] Referring to Figure 5, new material is acquired using a camera 50. A blank tape 51 is inserted into the camera 50. Also a smart card SC is inserted into an interface in the camera. This example assumes that the card is as shown in Figure 3 and has a processor SC1. The camera 50 produces image data (which may be DCT coefficients) which are applied to the processor in the card SC. The card applies the watermark defined by the stored template and the algorithm and keys. The card also generates one or more UMIDs to identify the material recorded on the tape. The UMIDs and keys so generated are stored in store SC5 on the card. The UMIDs are also recorded on the tape (see Figure 7 be-

low).

[0030] The card SC is removed from the camera 50 and inserted into the seller client 2. The data stored on the card is transferred to the server 1 via the network 4. In addition the seller may record on the smart card and transfer to the server 1 data such as price, and conditions of sale. In addition metadata relating to the material may be transferred. The UMIDs provide references which uniquely identify the material and the data associated with it which are transferred to the server 1.

Legacy Material, Figure 6.

[0031] Legacy material is "old " material which did not have a watermark applied according to the present invention when first acquired. Such legacy material may be stored on tape or in other storage 61, for example an A/V server 61. In the system of Figure 6, a VTR 62 has an interface for receiving a smart card SC and also a port for receiving material from the A/V server 61. Also an unwatermarked tape 60 containing legacy material may be inserted into the VTR 62. The VTR operating with the smart card SC applies a watermark and UMID to the legacy material and the generated keys and UMIDs are stored in the card SC as described above. The card SC is inserted into the seller client 2 for transfer, via network 4, of its data, plus any other data such a price and conditions of sale, as described above in relation to acquisition to the transaction server 1.

[0032] Figure 6 shows the VTR 62 and seller client as part of a Local Area Network having at least one workstation 2, 2'. That work station has an interface for receiving a smart card. Legacy material from the A/V store 61 may be routed to the workstation 2' which co-operates with the smart card to apply a watermark to the material which is then stored in the store 61. The UMIDs and keys generated during the process of watermarking are stored on the card SC. The workstation 2' may retrieve the data stored on the card and send it to the server 1. Watermarked material may be stored on the A/V server 61 and also on tape 60.

Tape, Figure 7.

[0033] Referring to Figure 7, an example of a tape 51 or 60 is shown. Watermarked Video is stored in conventional manner in helical tracks 70. The tape has a conventional control track 72 in which time codes are recorded. The UMIDs are recorded in the user bits of the time codes. That is described in more detail in copending British application 9926321.3,(also EP 00309067.7), attorney file P/7211, 1-99-41.

Transaction Server, Figure 8

[0034] The transaction server 1 provides secure communications with the seller and buyer clients. It also controls financial transactions by holding buyer and seller accounts. As described above, the seller registers passwords, bank account details with the server 1. In addition, the server provides algorithm specifications and registration, and provides a system for designing templates. It establishes rules for UMIDs. It also provides for the secure uploading and storage of keys and UMIDs generated during watermarking. Metadata may also be uploaded and stored in the server 1. The UMIDs provide references for associating the stored data with the material to which that data relates. The transaction server may provide to potential buyers access to the metadata. The access may be free of cost or subject to payment or a combination of both. The metadata may include clip lengths, time and data information amongst many other possibilities.

[0035] The transaction server may store multiple different algorithms for creating and removing watermarks, in addition to the currently preferred and inventive algorithm which is described in copending British application I-00- 147, P/10145, Application 0029850.5.

[0036] The transaction processor also monitors buyer interest and sales and controls the release of data for removing watermarks; such data is not released unless the server has confirmation that the buyer satisfies the conditions of sale including paying for the material.

[0037] The transaction server 1 also controls the distribution of smart cards.

Transaction Server, Figure 9

[0038] The transaction server also provides for the registration of data relating to the buyers. For example, the buyer provides details of bank accounts, passwords and any other data relevant to a transaction.

[0039] The registration of the buyer allows access to:

a) business rules, prices and conditions of sale to enable the buyer to purchase the material; and
b) data, such as metadata, relating to material received by the buyer and which the buyer has bought or which he might buy.

[0040] Once the buyer has satisfied the conditions of sale, the transaction server provides secure delivery of decryption keys, templates and algorithms for removing watermarks. That may be done by securely downloading data to smart cards as described above and sending the smart cards to the buyers.

Content Purchase, Figure 10.

[0041] Referring to Figure 10, a buyer receives watermarked material and previews it on a VTR 101. If the buyer is interested in the material, he accesses the UMID recorded on the tape and registers his interest in the material with the transaction server using the UMID as a reference via the buyer client 3 and the network 4. The transaction server provides to the buyer the condi-

tions of sale and price. If the buyer then agrees to buy, the buyer provides payment and requests the data needed to remove the watermark.

[0042] Payment may be by automatic transfer from his bank account previously registered with the server 1 or by other means which the server can monitor. Once the server 1 has confirmation of payment, the server 1 provides the watermark removal data. That data is downloaded via the buyer client 3 to a smart card SC as described above for example. The smart card is inserted into an interface in the VTR 101 which then co-operates with the card to remove the watermark. In this example the card is assumed to be a card as shown in Figure 3.

[0043] Instead of receiving watermarked material on tape or other recording medium, the watermarked material may be accessed from an A/V store 102.

[0044] The embodiments of the invention have been described with reference to video material. However the invention is also applicable to audio/visual material, to audio material and to other data material.

[0045] Whilst the foregoing refers to transferring material on tape via a physical communications network such as the Post, the material could be transferred via an electronic network, most preferably a broad-band network.

[0046] The network 4 may be the web as shown in the figures. It could be any other communication network.

[0047] Transfer of data between the server and the clients is preferably carried out in a secure manner using security techniques known in the art of secure communications.

Modifications.

[0048] The examples of the invention described above use a smart card for transferring data. The data may be transferred on other data carriers. Smart cards are advantageous because they provide security for the data. Data may be carried on other carriers preferably in encrypted form for security. Most preferably, the data carrier is hand insertable into an interface.

[0049] The transaction server contains metadata relating to the watermarked material. That metadata preferably includes samples and/or extracts of the watermarked material to allow potential buyers to browse the material available. For example for video, low resolution frames and/or video sequences may be browsed. The metadata also may include text describing the material which may be searched and which is also preferably linked to the samples of the material. Thus. for example a video sequence of a well known person may be accessed by searching for his or her name. Once found the buyer can request that the tape of the watermarked video be transferred to him.

[0050] The examples of the invention described above refer to video material. The invention may be applied to moving and still images. The invention may be applied to audio material or to data material. Preferably it is applicable to audio/visual material.

Second Example: client- server system-Figures 11 to 15.

Overview

[0051] Referring to Figure 11, a second example of a system in accordance with the invention comprises a transaction server 1, one or more seller clients 112, 112N, one or more buyer clients 113, 113N and a communications network 4 linking the clients to the server.

[0052] The owner of material, i.e. a seller, controls a seller client 112. A buyer controls a buyer client 113. A third party owns and controls the transaction server 1. The system allows material to be acquired, securely and visibly watermarked, and transferred to the buyer for the buyer to preview (9) the watermarked material. If the buyer then wants to buy the material, the buyer obtains the data needed to remove the watermark. In this example, the seller and buyer both register (10) with the transaction server. Registration, content preview, and watermark removal are described in more detail hereinbelow. The data for removal of the watermark is sent to the buyer only when the buyer has paid for the material. The payment is monitored by the transaction server 1 which communicates with a financial institution 8. Payment is made via the server 1 and/or via the institution 8.

[0053] The system of Figure 12 may be operated in two modes. In one mode, termed the "push mode" the seller sends tapes or other storage media to many potential buyers. The contents of the tapes are perceptibly watermarked allowing the potential buyers to view the content but the content is protected against misuse by the perceptible watermark. If a buyer decides to purchase, then he is sent removal data needed to remove the watermark.

[0054] In another mode, termed the "pull mode", potential buyers use metadata relating to the content stored on the transaction server to find content they are interested in and then request the seller to send them watermarked content for preview. If a buyer decides to purchase, then he is sent removal data needed to remove the watermark.

[0055] Referring to Figure 12, the seller obtains seller software, and registers with the transaction server. The seller client processor watermarks the material generating watermark removal data. The seller client processor informs the transaction server of watermark removal data and of identifiers associated with the material. The seller uses the client processor to provide metadata, rates card and business rules to the transaction server. The seller sends watermarked material to potential buyers. These steps will now be described in more detail.

Seller Registration-Figure 12

[0056] Someone who wishes to be a seller firstly ac-

quires seller software. This may be done in any conventional manner: for example by downloading it from the server 1, or by acquiring a stand alone software package. The seller registers with the server 1, providing to the transaction server 1 a) passwords, b) bank account details of the seller and c) any other information.

Apply watermark

[0057] The seller then needs to apply visible watermarks to the material he/she wishes to make available to buyers. In this example assume the material is a video sequence. The seller loads the material into the seller client to apply the watermark. The seller client is used to design and apply the watermark The seller client downloads from the transaction server watermark design software The seller uses the software off-line to design the form of the watermark and chooses parameters such as the perceptibility of the watermark as described hereinbelow. This results in watermark configuration data and removal data. The removal data is downloaded to the transaction server 1 and/or to a smart card as described above. The watermark configuration data is sent to a watermarking processor which in the preferred embodiment is in the seller client. The watermarked video may be stored on a storage medium 7 for example a tape, disc or solid state store. In this example the medium is a tape as shown in Figure 7.

[0058] The watermark is applied using an invertible algorithm which uses pseudo random numbers generated from one or more keys and one or more templates. An example of a suitable method of generating such a visible watermark is disclosed in copending UK applications 0029850.5, attorney file P/10145, I-00-147 and 0121197.8, P/10145GBP, I-00-147A the contents of which are incorporated herein by reference.

[0059] The seller may choose the level of the watermark, that is the perceptibility of the watermark. Thus a seller may mark particularly valuable material more heavily than other less valuable material. The area of a video frame covered by a watermark may be chosen. The watermark may vary with time through the material. Ways of doing that are disclosed in UK applications 0121197.8, attorney fileP/10145GBP, I-00-147A.

Apply identifier

[0060] An identifier is applied to the material. An example of an identifier is a Unique Material Identifier or UMID. UMIDs are described in more detail in SMPTE Journal March 2000. The UMID is generated in the seller client 112. One or more UMIDs may be applied to a video sequence. A UMID uniquely identifies the video sequence to which it applies. The UMID may be applied as an invisible watermark and/or may be stored on the storage medium 7 with the video as shown in Figure 7. Alternatively, the UMID may be attached to, or otherwise associated with, the storage medium.

[0061] The seller client processor 112 informs the transaction server 1 of the algorithm, key(s), template (s), used to generate the watermark and of the UMID(s) applied to the video sequence.

[0062] The seller also provides, to the transaction server 1, metadata, rates card data, business rules data and data for a license file. This data is provided by interacting with the transaction server and will be described with reference to Figure 14.

Metadata-Figure 14A

[0063] In this example the seller provides: a) some metadata (free metadata) which is useable by buyers free of charge, mainly so potential buyers can browse material which is for sale; and b) other metadata which is available only if paid for. The metadata includes identifiers, preferably the UMID(s), which are required to associate the metadata with the material. Metadata may be generated at the seller client 112 and/or by a separate generator (115 in Figure 11). The generator 115 may be provided by an independent organisation who specialises in generating metadata.

[0064] The free metadata comprises metadata which allows buyers to find material which interests them and to determine whether they wish to preview it in more detail. Thus for an image or a video sequence the free metadata may comprise one or more small picture stamps, and keywords which allow buyers to search for material by descriptive words. The free metadata may also include for example the resolution of the image and other data.

[0065] Other free metadata, which may be invisible to the buyer, may include the IP (Internet Protocol) or other address of the seller client. The UMID(s) may be invisible to the buyer.

[0066] The metadata for which the buyer must pay may include for example data such as the script of a video sequence and other artistically creative data which may be intellectual property which is not owned by the owner of the video sequence. It may include metadata generated by the independent organisation and for which the seller wishes to recoup the cost of generation.

Rates Card-Figure 14B

[0067] The rates card is a list of the prices at which the seller is willing to sell material the seller is offering. The rates card is preferably not accessible to buyers. Preferably the buyer is given only a final price for the use he wishes to make of the material. That price is determined on the basis of the rates card and the buyers responses to questions about his/her intended use.

[0068] The rates card may set a single price, or a set of prices for different conditions of sale.: A single rates card may be set up for all, or groups of, material offered by a seller. Alternatively, separate rates cards may be

provided for respective items of material which cards are referenced to the material by the material identifiers, e. g. UMIDs.

[0069] By way of example a rates card for a video sequence may set

- A base price of cost per second of video and adjustments of that base price for:-.
- outright sale,
- use once on broadcast television,
- multiple use on broadcast television,
- for duplication and distribution on video tape or disc,
- Price variation dependent on the resolution of the video which is to be distributed, and/or
- some uses or some multiple uses or repeat business.

The rates card may set any other organisation of prices.

[0070] The rates card may provide a seller with a predetermined set of prices which may be based on the experience of the operator of the transaction server in the market the operator serves. However, preferably the transaction server allows the seller to set up their own pricing.

Business Rules-Figure 14C

[0071] The server 1 may store one or more predetermined, standard contracts and/or may provide a seller with the facility to set their own customised terms of contract. The contract once set by the seller is accessible by buyers.

Buyer Registration- Figure 13

[0072] Someone who wishes to be a buyer, firstly acquires buyer software. This may be done in any conventional manner: for example by downloading from the server 1, or by acquiring a stand alone software package. The buyer registers with the server 1, providing to the transaction server 1 a) passwords, b) bank account details of the buyer and c) any other information.

Buyer searches for video of interest-Figure 13.

[0073] The buyer accesses the metadata stored on the transaction server to look for video which interests him using for example key words. The buyer also accesses for example picture stamps. If the buyer finds video which may interest him he then expresses an interest in the video sequence. The transaction server 1 informs the seller client 112 and a visibly watermarked copy is sent to the buyer. In a currently preferred example, the copy is sent to the buyer on the storage medium, e.g. a tape 7 by post or courier. However it could be sent in other ways; for example electronically via the network 4 especially if the network supports 'broad-band' transmission of video. The transaction server 1 may automatically send an e-mail to the seller client to inform the seller of the buyers interest and to prompt them to send the video to the buyer. Alternatively, the request could be processed by an automated warehouse (117 in Figure 11) in response to an order from the server 1 or the client 112. The warehouse 117 would dispatch a storage medium 7 containing the desired video to the buyer.

[0074] The interest of the buyer is registered with a transaction log.

[0075] The following description assumes the buyer stores the video electronically in a storage medium associated with his client processor 113.

The buyer pays for the video and removes the watermark.

[0076] The buyer reviews the watermarked copy. If he wishes to buy it he indicates his interest. The buyer client 113 identifies the video from the identifier (UMID) associated therewith. The identifier is transmitted to the transaction server 1. The server then allows him to access the business rules and the rates card to determine the price and the conditions with which he must comply. The buyer may also buy additional metadata. He may pay electronically via the network 4. The payment and the identifier of the video is registered with the transaction log. A license file is generated and stored at the transaction server. The file contains the data set out with reference to Figure 14D.

License file-Figure 14D

[0077] Once payment has been acknowledged by the transaction server, the licence file is downloaded from the transaction server to the buyer client. The file contains the UMID(s), the free metadata , the bought metadata, the business rules, the price information, and the secret data for removing the watermark. The file may also include secret security data for adding a fingerprint to the material. The visible watermark is removed using the removal data in the license file and preferably an invisible fingerprint is added. The fingerprint uniquely identifies the buyer to help protect the video against unauthorised use. The fingerprint allows the owner of the material to trace misused video back the buyer.

[0078] The removal of the visible watermark and the addition of the fingerprint take place in the buyer client, which may be a PC, securely without interaction by the buyer. The software required to do that is protected by known digital rights management techniques against misuse.

Statistics and transaction log- Figure 15.

[0079] Referring to Figure 15, the transaction server 1 preferably maintains a transaction log, which contains for each seller statistical data useful to the sellers. For example the log may contain the identity of each seller

and for each seller the following data:-

Identities of buyers;
Identification of the content (material) sold;
The price;
Total sales;
Analysis of sales by genre;
Analysis of sales by country or /region; and/or
Details of material for which a user license has expired.

Modifications

[0080] Various modifications may be made to the second example.

[0081] The second example has been described with reference to a server-client system in which the server stores the material and provides the interfaces between it and the clients for registering sellers and buyers and for designing watermarks and for financial transactions. However, the present invention may be applied in the context of a peer to peer network in which at least the material is stored on many stores, e.g. 112S. For example each seller may store their own material and a server (such as server 1) acts to provide general organisation of the network.

[0082] This peer to peer network structure is preferably used in the pull mode discussed above. That is potential buyers use metadata relating to the content stored on the server 1 to find content they are interested in. The buyer may access the watermarked material directly from storage associated with the seller client processor 112 via the network 4. Alternatively the buyer may be sent a watermarked tape to preview. If a buyer decides to purchase, and pays for the material then he is sent the license file including the removal data needed to remove the watermark.

[0083] Whilst the second example uses interfaces via which sellers and buyers must register manually to offer material for sale and to buy it, the present invention may provide an automatic registration and purchase of material via a "transparent " interface. For example, a trusted organisation such as a major broadcaster has an account with a seller to access material from them. The terms of sale of material are agreed in advance with the seller. The broadcaster is provided with a pre-configured ID on a secure store for example a smart card which identifies the broadcaster to the system. A video editor employed by the broadcaster uses the system of the second example to access a video clip which he requires without the need to register; that is done automatically when he chooses a clip to be downloaded to him. The clip is downloaded with the license file containing the secret removal data enabling the watermark to be removed from the clip (and also the fingerprint added to it).

[0084] In any of the examples set out above, the material may be robustly and invisibly watermarked before it is visibly watermarked.

[0085] Whilst the invention has been described with reference to video, it may be applied to audio. An audible distortion is added to the audio but the distortion allows a listener to appreciate what the audio signal represents. The distortion is robust against unauthorised removal but is removable to restore the original audio.

[0086] The seller client may interact on-line with the transaction server to create the watermark.

Claims

1. A method of watermarking and transferring watermarked material in a system comprising a transaction server, first and second clients, first apparatus for applying a perceptible watermark to the material and second apparatus for removing the watermark; the method comprising the steps of:

   transferring from the transaction server to the first apparatus (i) data for creating a watermark, the creating data including (a) data defining an invertible algorithm and (b) data for creating at least one security key associated with the algorithm and (ii) data for creating a material identifier;
   using the said first apparatus to apply a material identifier to the material and applying a watermark to the material, using the said creating data;
   transferring from the first client to the transaction server the said material identifier and data for inverting the algorithm including the said at least one key;
   transferring the watermarked material to the second apparatus;
   deriving the said material identifier from the material;
   transferring the identifier from the second client to the transaction server;
   subject to predetermined conditions being satisfied, transferring from the transaction server to the second apparatus watermark removal data associated with the said material identifier, the removal data including at least one key and data defining an algorithm for removing the watermark in conjunction with the key; and
   using the second apparatus to remove the watermark using the said removal data.

2. A method according to claim 1, wherein the first apparatus compresses the material and applies the watermark as part of the compression process.

3. A method according to claim 1, or 2, wherein the said data defining the invertible algorithm comprises algorithm configuration data.

4. A method according to claim 1, 2 or 3, wherein the said data defining the invertible algorithm comprises the algorithm.

5. A method according to claim 1, 2, 3, or 4, wherein data for creating the material identifier is stored in a data carrier for transfer to the first apparatus.

6. A method according to claim 1, 2, 3, 4 or 5, wherein the said data for creating a watermark is stored in a data carrier for transfer to the first apparatus.

7. A method according to claim 6, wherein a material identifier and at least one key are generated during the application of the watermark to the material, and comprising the step of storing the generated identifier and key on a data carrier for transfer to the first client for transfer to the transaction server.

8. A method according to any preceding claim, comprising the step of storing in the transaction server metadata relating the said watermarked material, the metadata being referenced by the said identifier.

9. A method according to any one of claims 1 to 8, wherein the said removal data is stored in a data carrier for transfer to the second apparatus.

10. A method according to any preceding claim, comprising storing on the transaction server conditions of sale of unwatermarked material.

11. A method according to claim 10, comprising the step of transferring the said conditions of sale from the first client to the transaction server.

12. A method according to claim 10 or 11, wherein the transaction server transfers the said removal data subject to the condition that a buyer has fulfilled the conditions of sale.

13. A method according to any preceding claim, comprising the step of storing the watermarked material in a recording medium and transferring the watermarked material to the second apparatus on the recording medium.

14. A data carrier in which is stored (i) data for creating a watermark, the creating data including (a) data defining an invertible algorithm and (b) data for creating at least one security key associated with the algorithm and (ii) data for creating a material identifier.

15. A data carrier according to claim 14, wherein the carrier is a smart card comprises a processor and memory and the processor is programmed to implement the said algorithm.

16. A data carrier according to claim 14, wherein the carrier is a smart card comprises memory storing algorithm configuration data defining the invertible algorithm.

17. A data carrier in which is stored watermark removal data including at least one key and data defining an algorithm for removing a watermark in conjunction with the key.

18. A data carrier according to claim 17, wherein the carrier is a smart card comprises a processor and memory and the processor is programmed to implement the said algorithm.

19. A data carrier according to claim 17, wherein the carrier is a smart card comprises memory storing algorithm configuration data defining the invertible algorithm.

20. A system comprising a transaction server, first and second clients, first apparatus for applying a perceptible watermark to the material and second apparatus for removing the watermark, the said first and second clients, first apparatus for applying a perceptible watermark to the material and second apparatus for removing the watermark being linked by one or more communications networks; the system being arranged to implement the method of any one of claims 1 to 13.

21. A method or system according to any preceding claim wherein the said material is video material.

22. A method or system according to any one of claims 1 to 20 wherein the said material is audio/visual material.

23. A method or system according to any one of claims 1 to 20 wherein the said material is audio material.

24. A method or system according to any one of claims 1 to 20 wherein the said material is data material.

25. A data processing apparatus comprising

an information material processing apparatus operable to receive signals representative of information material, and to adapt said signals to the effect of introducing a reversible modification to said information material in accordance with a modification key, said modification being arranged to provide a disturbing effect on the information material to a human recipient,

a data generation processor operable to generate data identifying said information material,

a recording apparatus operable to record said adapted signals and said identifying data on a recording/reproducing medium, and

a data processor operable to receive said identifying data and said modification key and to store said identifying data and data representative of said modification key data on a data carrier.

26. An apparatus as claimed in Claim 25, wherein said recording/reproducing medium is a linear recording medium including capacity for ancillary data, and said identifying data is recorded in said capacity for recording ancillary data.

27. An apparatus as claimed in Claim 25 or 26, wherein said data carrier is a hand insertable carrier.

28. An apparatus as claimed in Claim 27, wherein said data carrier is a smart card or the like.

29. An apparatus as claimed in any of Claims 25 to 28, wherein said identifying data is a Unique Material Identifier or the like.

30. An apparatus as claimed in any one of Claims 25 to 29, said apparatus comprising .

an information material server arranged to store signals representative of information material, and to retrieve selected signals representative of selected information material items, said information material processing apparatus being operable to adapt said selected signals, said data generation processor being operable to generate said data identifying said selected information material signals.

31. A camera comprising the apparatus according to any of Claims 25 to 30.

32. An apparatus for receiving a data carrier having data stored by the apparatus according to any of Claims 25 to 31, said apparatus comprising

a data reading processor operable to receive said data carrier via hand insertion by a user and to read the modification key and the identifying data, and

a communications processor operable to communicate said modification key and said identifying data to a data base processor.

33. An apparatus as claimed in Claim 32, wherein said communications processor is operable to communicate said modification key and said identifying data to said data base processor via a communications network.

34. An apparatus as claimed in Claim 33, wherein said communications network is the Internet.

35. An apparatus as claimed in any of Claims 32 to 34, wherein said communications processor is operable to receive data representative of sales conditions and price information and to communicate said sales conditions and said price information with said modification key data and said identifying data to said data base processor.

36. A signal bearing the modification key and the identifying data generated by the apparatus according to any of Claims 32 to 35.

37. A signal ensemble comprising the adapted signals representing audio and/or video signals adapted by the apparatus as claimed in any of Claims 25 to 31, and the signal bearing the modification key and the identifying data generated by the apparatus according to any of Claims 32 to 36.

38. A method comprising the steps of:

applying, using a watermarking apparatus, a removable perceptible watermark to material, the watermark being removable using removal data created during application of the watermark and applying identifying data to the material to identify the watermarked material;
registering with a transaction server conditions for the removal of the watermark and identifying data identifying the watermarked material;
transferring the watermarked material to a watermark removal apparatus; and
identifying to the server the transferred material, and transferring the removal data to the removal apparatus to allow removal of the watermark if the transaction server indicates that predetermined conditions for removal are satisfied.

39. A method according to claim 38, wherein the said conditions are conditions of sale of the material.

40. A method according to claim 39 wherein the conditions of sale include paying for the material.

41. A method according to claim 38 or 39 or 40, comprising the step of using a first client linked to the transaction server by a communications network to register the said conditions.

42. A method according to claim 41. comprising the step of using a second client linked to the transaction server by a communications network to comply with the said conditions.

43. A method according to any one of claims 38 to 42, comprising the steps of loading the removal data onto a data carrier and transferring the carrier to the removal apparatus when the said conditions are satisfied.

44. A method according to claim 43, wherein the removal data is downloaded onto the data carrier from the transaction server via the communications network.

45. A method according to claim 44, wherein the data carrier is a smart card.

46. A system comprising a watermarking apparatus, a transaction server and a watermark removal apparatus arranged to carry out the method of any one of claims 38 to 45.

47. A server arranged to:

a) receive and store data identifying watermarked material, data enabling removal of the watermarks from material and data setting predetermined conditions for the removal of watermarks; and
b) receive identifying data identifying watermarked material form which a watermark is to be removed;
c) monitor whether the predetermined conditions are satisfied; and
d) if the conditions are satisfied, providing the removal data for transfer to apparatus for removal of the watermark.

48. A server according to claim 47, wherein the said predetermined conditions are conditions of sale of the material.

49. A server according to claim 48, arranged to receive and store financial data relating to the sellers of the watermarked material.

50. A server according to claim 48 or 49, arranged to receive and store financial data relating to buyers of the watermarked material.

51. A server according to claim 48, 49 or 50, wherein the said conditions of sale include paying for the material.

52. A server according to claim 51, wherein the server is arranged to monitor transfer of money from the buyer to the seller.

53. A server according to claim 52, which is linked by a communications network with a financial institution to monitor the said transfer of money.

54. A server according to any one of claims 47 to 53, wherein the removal data includes a template and a security key.

55. A server arranged to:

interact with a client so as to enable a user of the client to design a template of a watermark; and
output a watermarking algorithm, or data for configuring such an algorithm, and data for generating security keys for implementing the algorithm.

56. A server according to claim 55, arranged to output the said algorithm or configuring data and the key generating data to a data carrier for transfer to the said user.

57. A server according to claim 56, wherein the data carrier is a smart card.

58. A data processing apparatus arranged to :

a) transfer, to a server via a communications network, data identifying watermarked material and a request for removal data enabling the removal of the watermark from the identified material; and
b) receive the removal data.

59. Apparatus according to claim 58, comprising an interface for receiving a data carrier, the apparatus being arranged to transfer the removal data to the carrier when the carrier is received by the interface.

60. A system according to claim 58, further comprising a store storing watermarked material, the apparatus being arranged to receive the said material from the store, and to remove the watermark using the said removal data.

61. A system according to claim 60, arranged to store the material from which the watermark has been removed in the said store.

62. Apparatus for removing a watermark from watermarked material, comprising:

a first port for receiving the said watermarked material; and
a second port for receiving watermark removal data.

63. Apparatus according to claim 62, wherein the first port is arranged to receive a first data carrier on which the said material is recorded; and
the second port is arranged to receive a second data carrier on which the said removal data is recorded.

64. Apparatus according to claim 63 wherein the second port is arranged to receive a smart card.

65. Apparatus according to claim 63 or 63 wherein the first port is arranged to receive a tape record.

66. A watermark removal system comprising apparatus any one of claims 62 to 65 and an apparatus or system according to any one of claims 58 to 61.

67. A signal comprising watermark removal data including a key and an algorithm or data for configuring an algorithm.

68. A signal according to claim 67, further including a watermark template.

69. A signal ensemble comprising a signal according to claim 66, 67 or 68 and a separate signal including the watermarked material.

70. A method comprising the steps of:

receiving, via a first channel, material which is watermarked with a watermark which is reversible; and
receiving, via a second channel, removal data which enables the removal of the watermark.

71. A method according to claim 70, wherein the first and second channels follow different paths.

72. A method according to claim 70 or 71, further comprising the step of removing the watermark using the removal data.

73. A method of watermarking and transferring watermarked material in a system comprising a transaction server and at least first and second clients, the method comprising the steps of:

using the first client to (i) create a watermark, defined by (a) an invertible algorithm and (b) at least one security key associated with the algorithm and (ii) provide a material identifier;
using the said first client to associate the material identifier with the material and apply the watermark to the material;
and storing, in the transaction server, the said material identifier and data for inverting the algorithm including the said at least one key;
transferring the watermarked material to the second client;
deriving the said material identifier associated with the material;
transferring the identifier from the second client to the transaction server;
subject to predetermined conditions being satisfied, transferring from the transaction server to the second client watermark removal data associated with the said material identifier, the removal data including at least one key and data defining an algorithm for removing the watermark in conjunction with the key; and
using the second client to remove the watermark using the said removal data.

74. A method according to claim 73, wherein the watermarked material is transferred to the second client via a communications channel.

75. A method according to claim 73, comprising the step of storing in the transaction server metadata relating the said watermarked material, the metadata being referenced to the material by the said identifier.

76. A method according to claim 73, 74 or 75, comprising storing on the transaction server financial rules relating to use of the material.

77. A method according to claim 76, wherein the financial rules are referenced to the material by the said identifier.

78. A method according to claim 73, 74, 75, 75 or 77, comprising storing on the transaction server business rules relating to use of the material.

79. A method according to claim 73, 74, 75, 7, 77 or 78, comprising storing on the transaction server statistical data relating to transactions associated with the material.

80. A method according to any one of claims 73 to 79, comprising creating at the transaction server files associated with respective items of material which users have been allowed to use by virtue of a business transaction.

81. A method according to claim 80, each file containing data relating to the rules of the business transaction.

82. A method according to claim 80 or 81, wherein each file contains metadata relating to the item of material.

83. A method according to claim 80 or 81, wherein each file contains the removal data.

84. A method according to claim 83 wherein the removal data is secured against unauthorized access thereto.

85. A method according to any one of claims 80 to 84, wherein the transaction server transfers the said file to the second client.

86. A method according to claim 84, when dependent on claim 83 or 84, wherein the step of transferring removal data comprises transferring the said file to the second client.

87. A method according to any one of claims 73 to 86, comprising the step of storing the watermarked material in a recording medium and transferring the watermarked material to the second client on the recording medium.

88. A method according to any one of claims 73 to 87, wherein the first client downloads watermark creation software from the server to create a watermark off-line.

89. A method according to any one of claims 73 to 87, wherein the first client interacts with the transaction server to create the watermark.

90. A system comprising a transaction server and first and second clients, the system being arranged to implement the method of any one of claims 73 to 99.

91. A method or system according to any one of claims 73 to 90 wherein the said material is video material.

92. A method or system according to any one of claims 73 to 90 wherein the said material is audio/visual material.

93. A method or system according to any one of claims 73 to 90 wherein the said material is audio material.

94. A method or system according to any one of claims 73 to 90 wherein the said material is data material.

95. A suite of computer programs containing instructions which when run on a system comprising a server and first and second clients configures the system to operate according to the method of any one.of claims 73 to 89 and 91 to 94.

96. A computer program product arranged to implement the method of any one of claims 1 to 13 and 21 when run on a system comprising a transaction server, first and second clients first apparatus for applying a perceptible watermark to the material and second apparatus for removing the watermark.

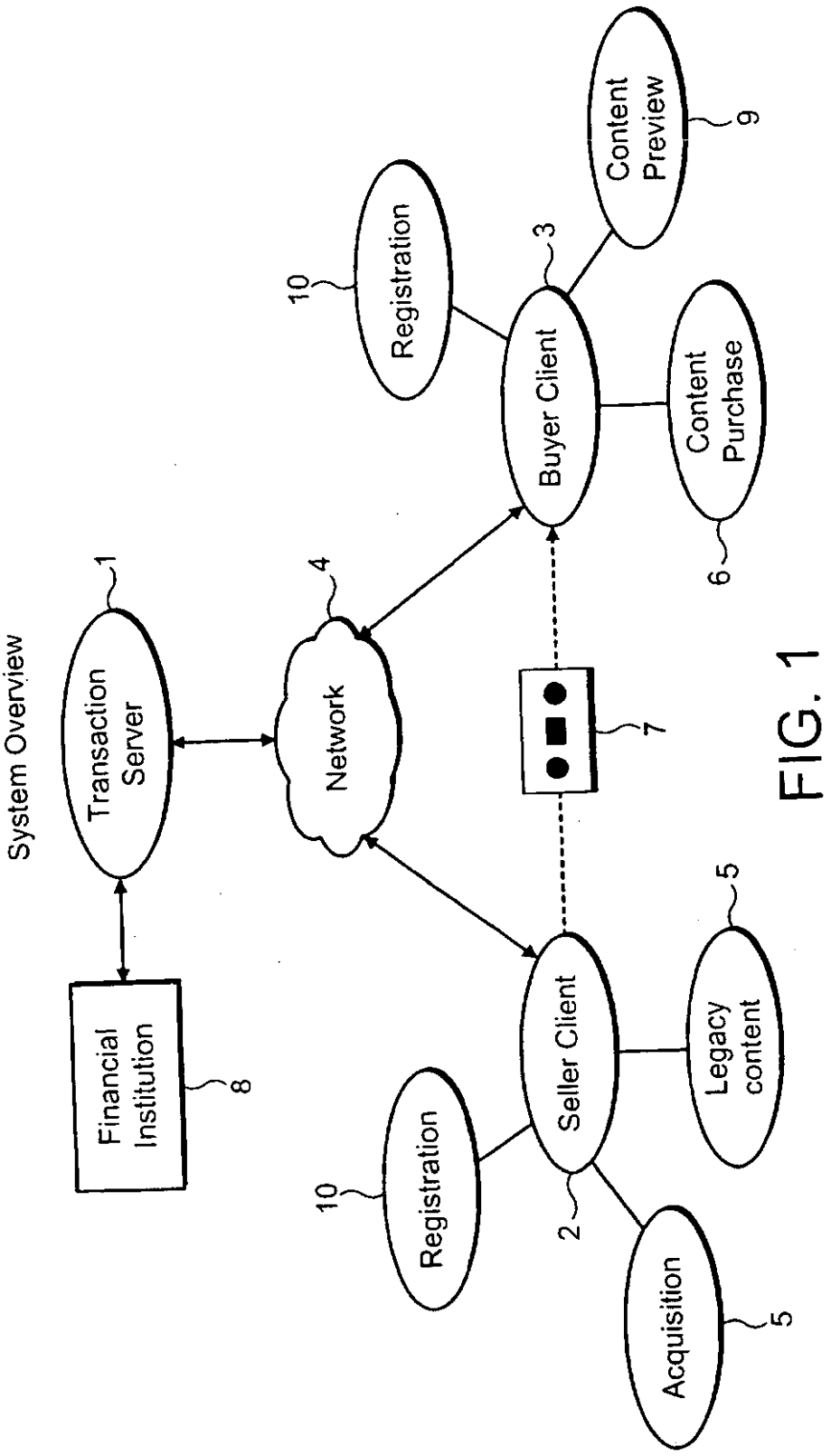
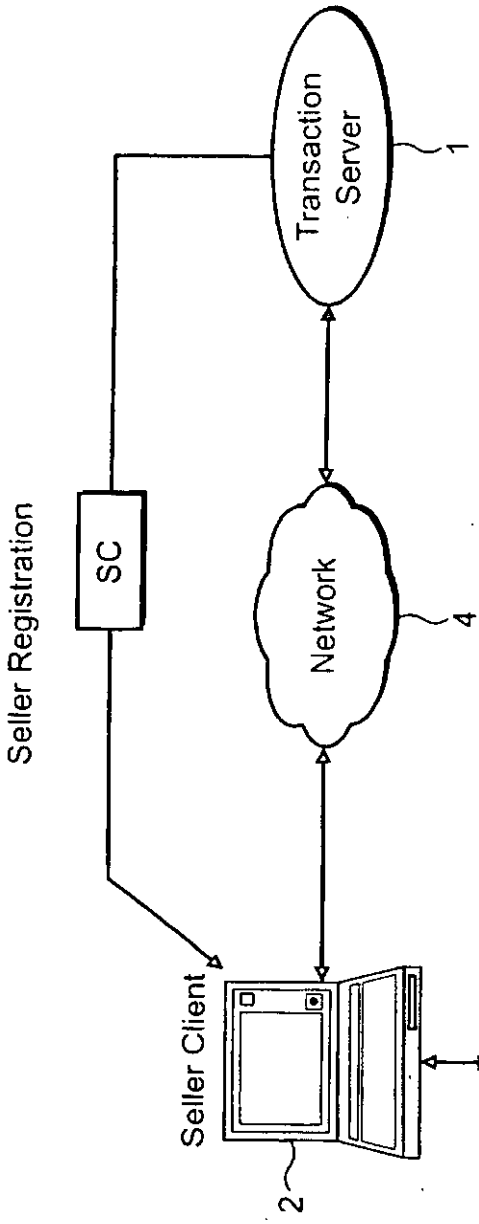

System Overview
Transaction Server
1
Financial Institution
8
Network
4
Registration
10
Buyer Client
3
Content Preview
9
Content Purchase
6
7
Registration
10
Seller Client
2
Legacy content
5
Acquisition
5

FIG. 1



- Seller registers with transaction-server, setting passwords, bank account details etc.
- Transaction-server sends smart-card to seller
- Seller designs template and chooses algorithm using the transaction server web-site
- Seller's smart-card is configured

FIG. 2

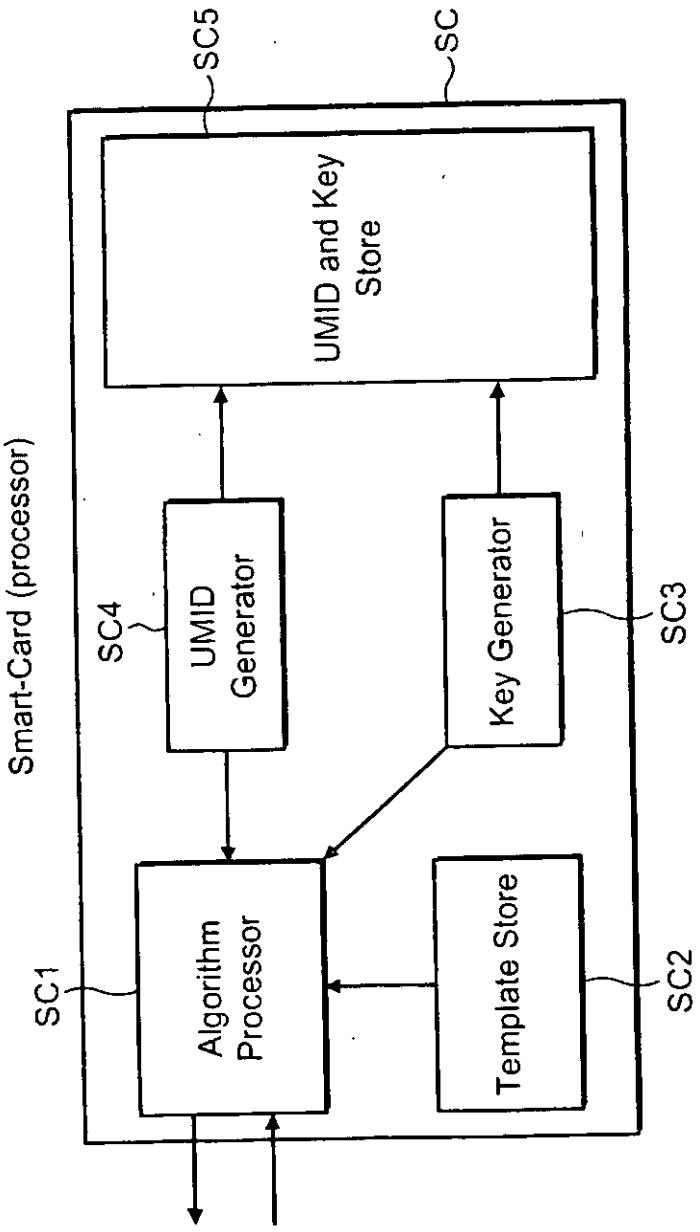


FIG. 3

All algorithmic processing, key generation and UMID generation is performed on the smart-card

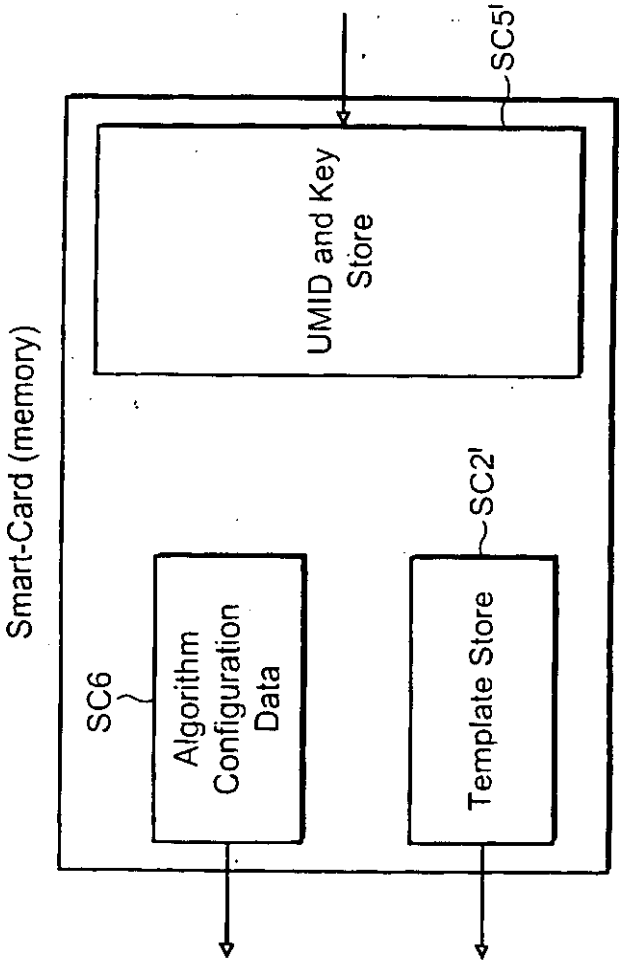

Smart-Card (memory)
SC6
Algorithm Configuration Data
Template Store
SC2'
UMID and Key Store
SC5'
·Smart-card initialised with algorithm configuration data and template
· Generated UMIDs and keys are loaded onto the smart-card

FIG. 4

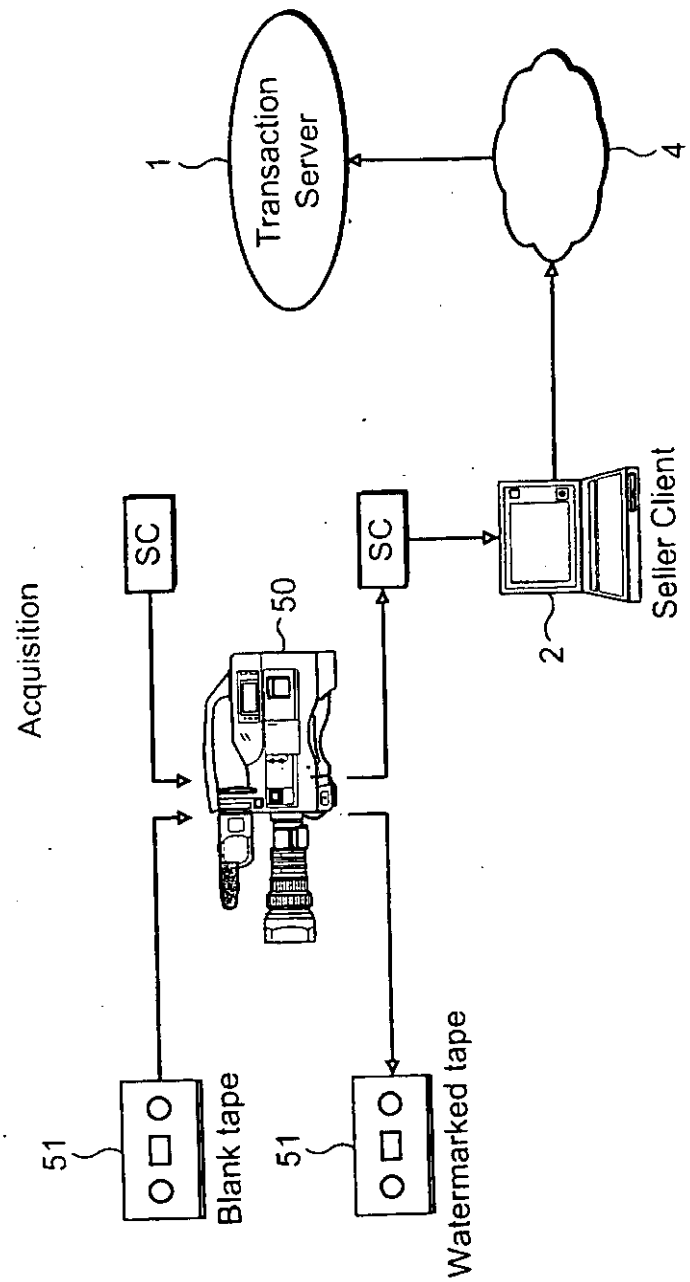


FIG. 5

·Upload transaction-server with UMIDs, keys, metadata, price information, conditions-of-sale, etc

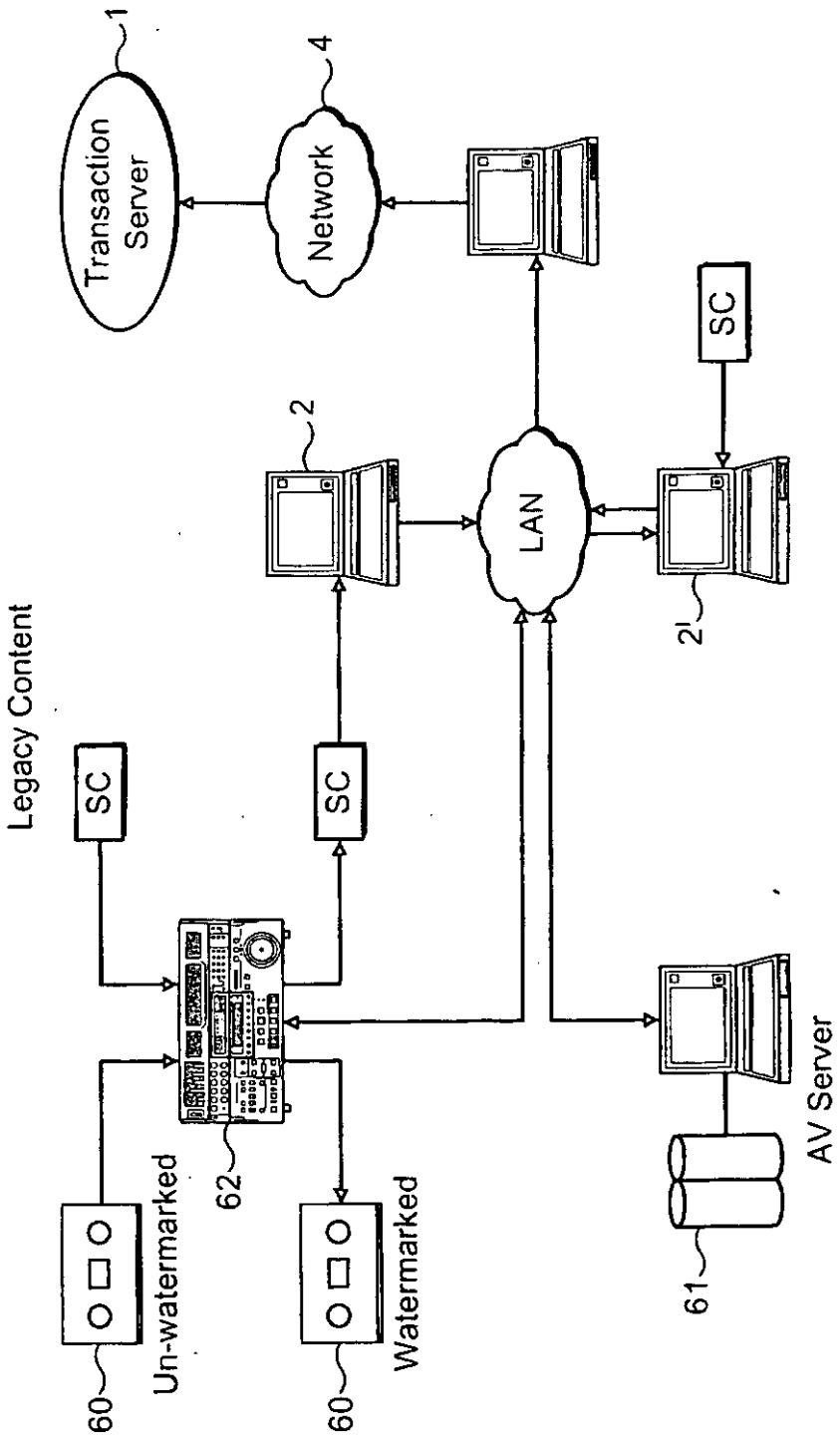

Transaction Server
1
Network
4
LAN
2
2'
SC
SC
SC
Legacy Content
Un-watermarked
Watermarked
60
60
62
61
AV Server
· Upload transaction-server with UMIDs, keys, metadata, price information, conditions of sale, etc

FIG. 6

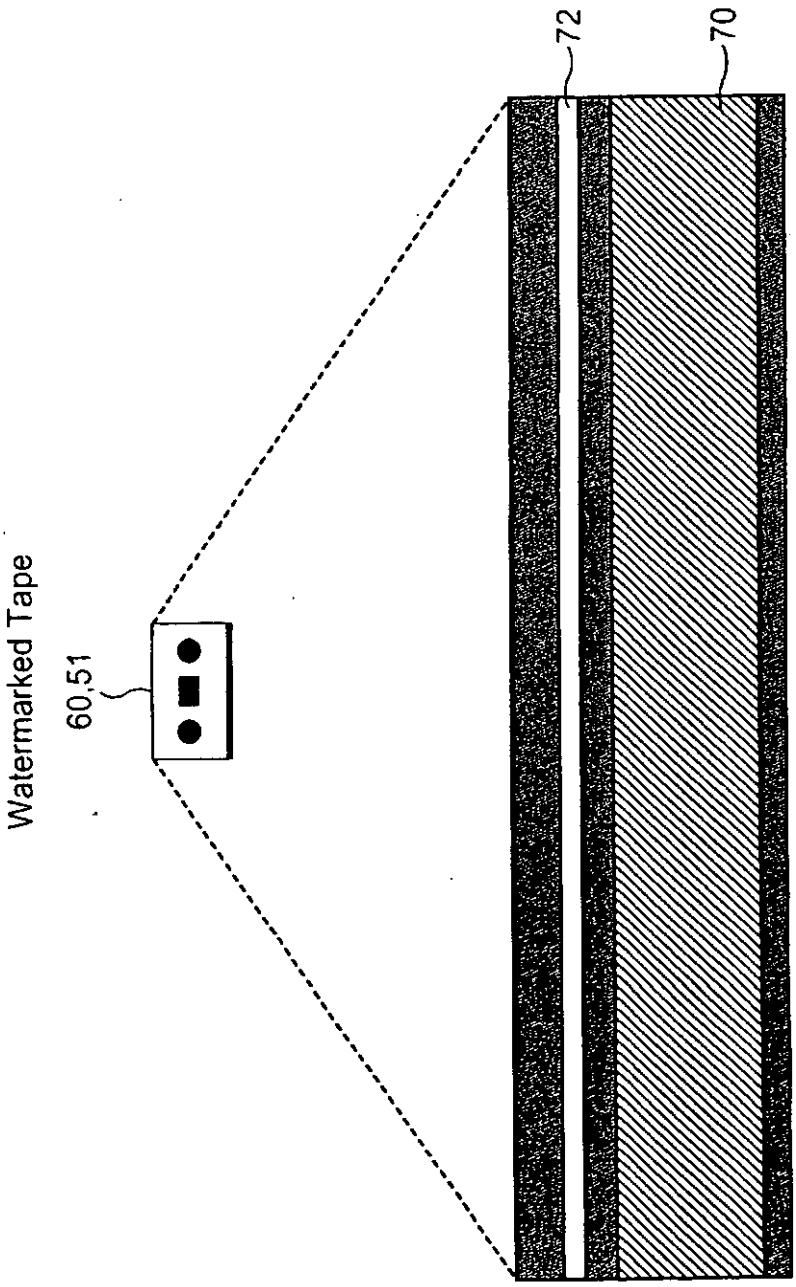
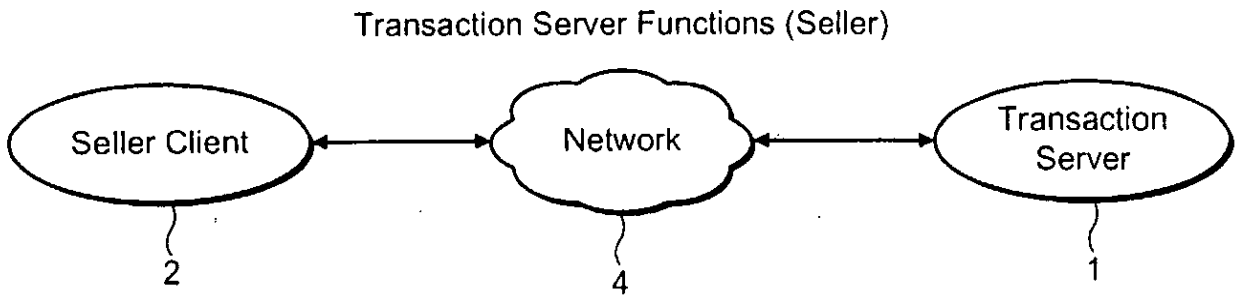


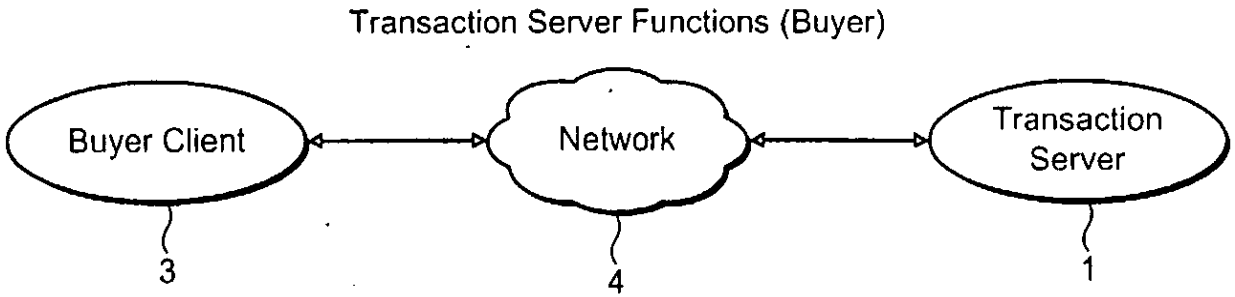
FIG. 7



- Seller registration (approval, passwords, bank account details etc.)
- Visible watermark template design, validation and registration
- Algorithm specification and registration
- Establish business rules for UMIDs
- Publish metadata (clip-length, time & date etc.)
- View / monitor buyer interest and sales
- Secure upload of keys and UMIDs for watermarked content (SSL)

FIG. 8

EP 1 215 907 A2



- Buyer registration (approval, passwords, bank account details etc.)
- Access to metadata
- Register interest in UMIDs
- Access business rules and pricing - enable purchase
- Secure delivery of decryption-keys, templates and algorithms (SSL)

FIG. 9

EP 1 215 907 A2

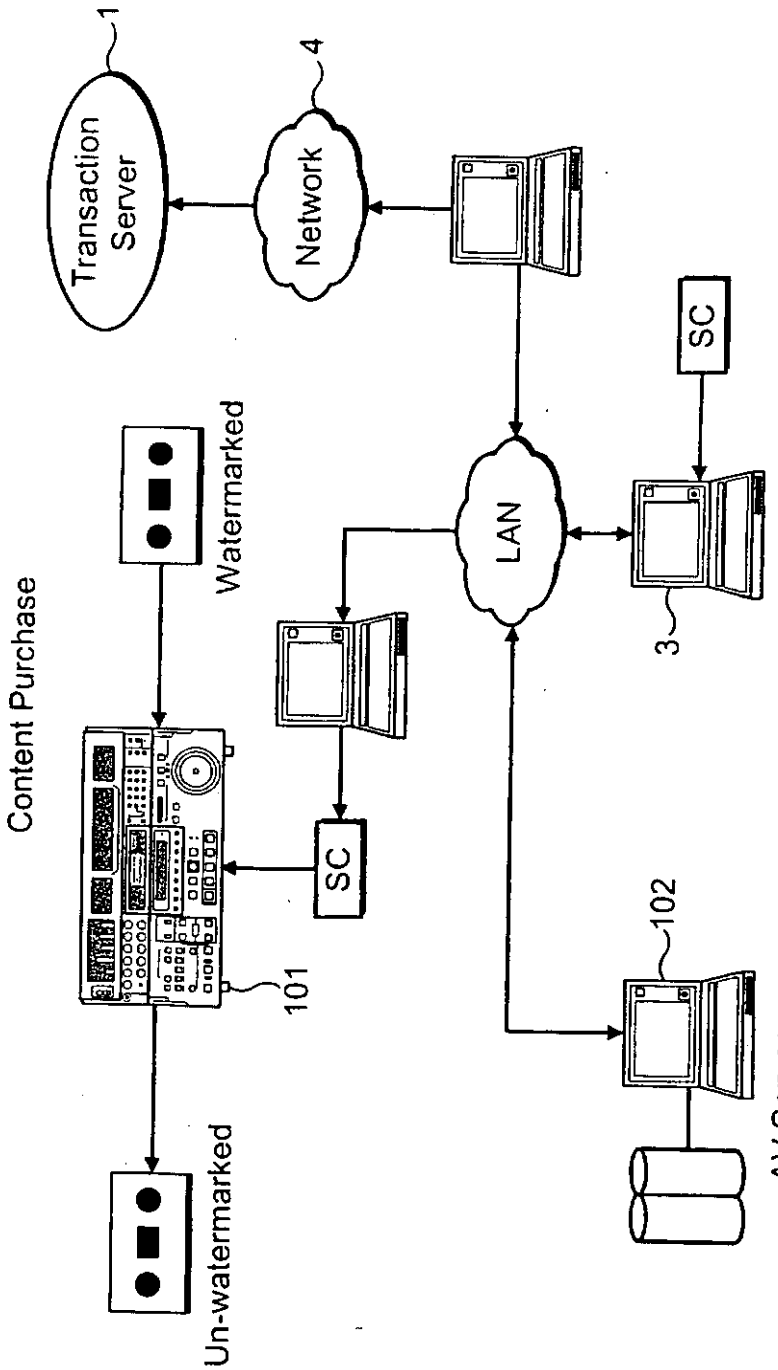

1
Transaction Server
4
Network
SC
Watermarked
LAN
Content Purchase
3
SC
101
102
Un-watermarked
AV Server

FIG. 10

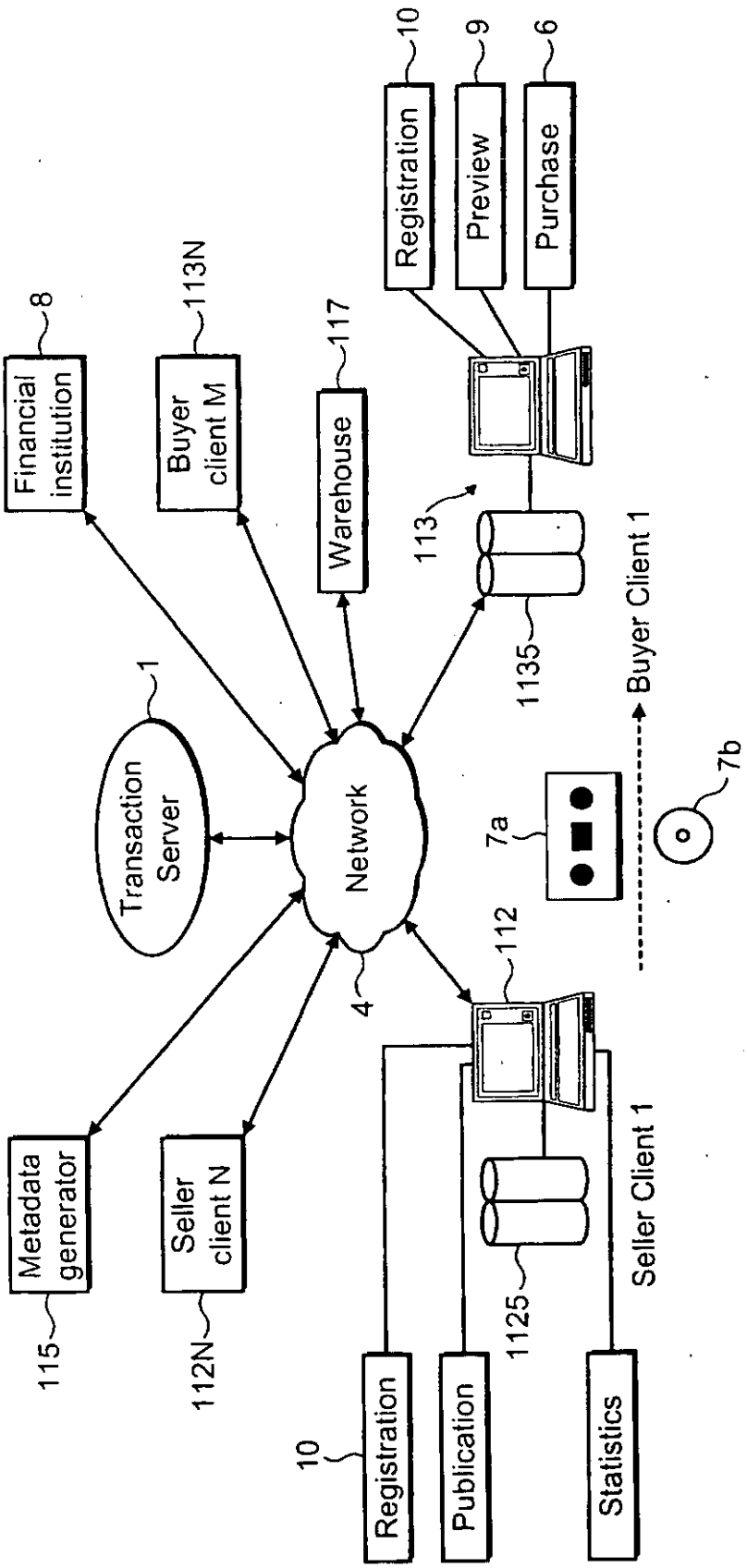

Registration
10
Preview
9
Purchase
6
Financial institution
8
Buyer client M
113N
Warehouse
117
113
1135
Buyer Client 1
Transaction Server
1
Network
4
7a
7b
112
Metadata generator
115
Seller client N
112N
1125
Seller Client 1
10
Registration
Publication
Statistics

FIG. 11

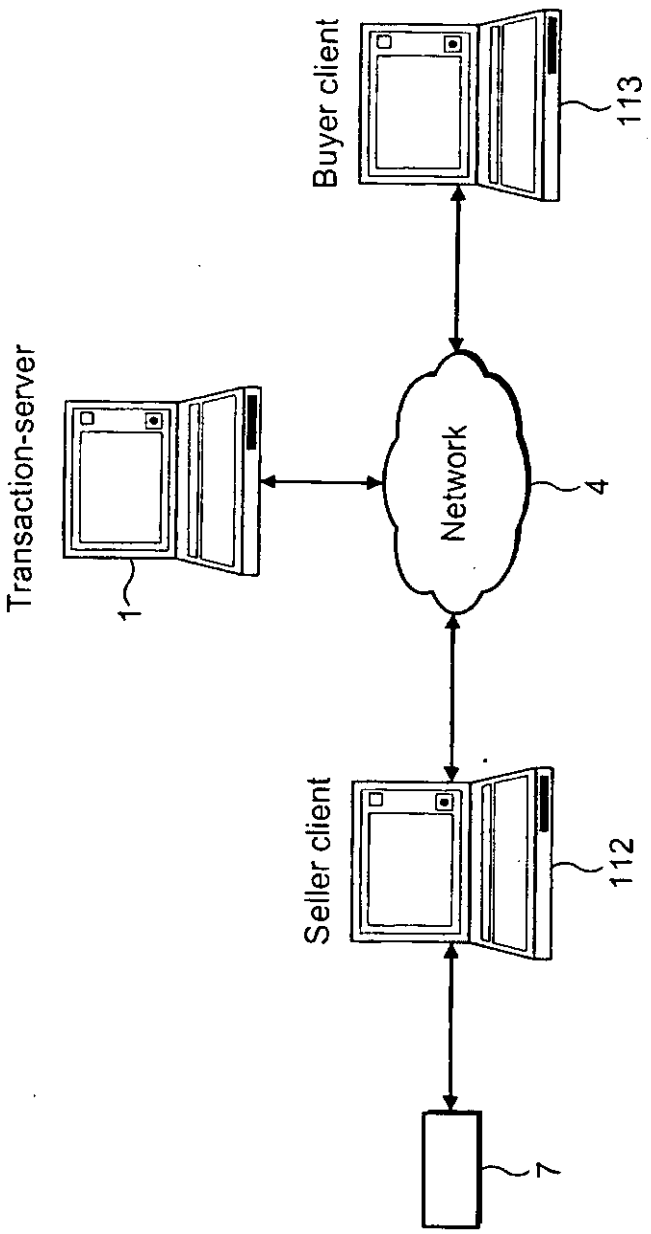
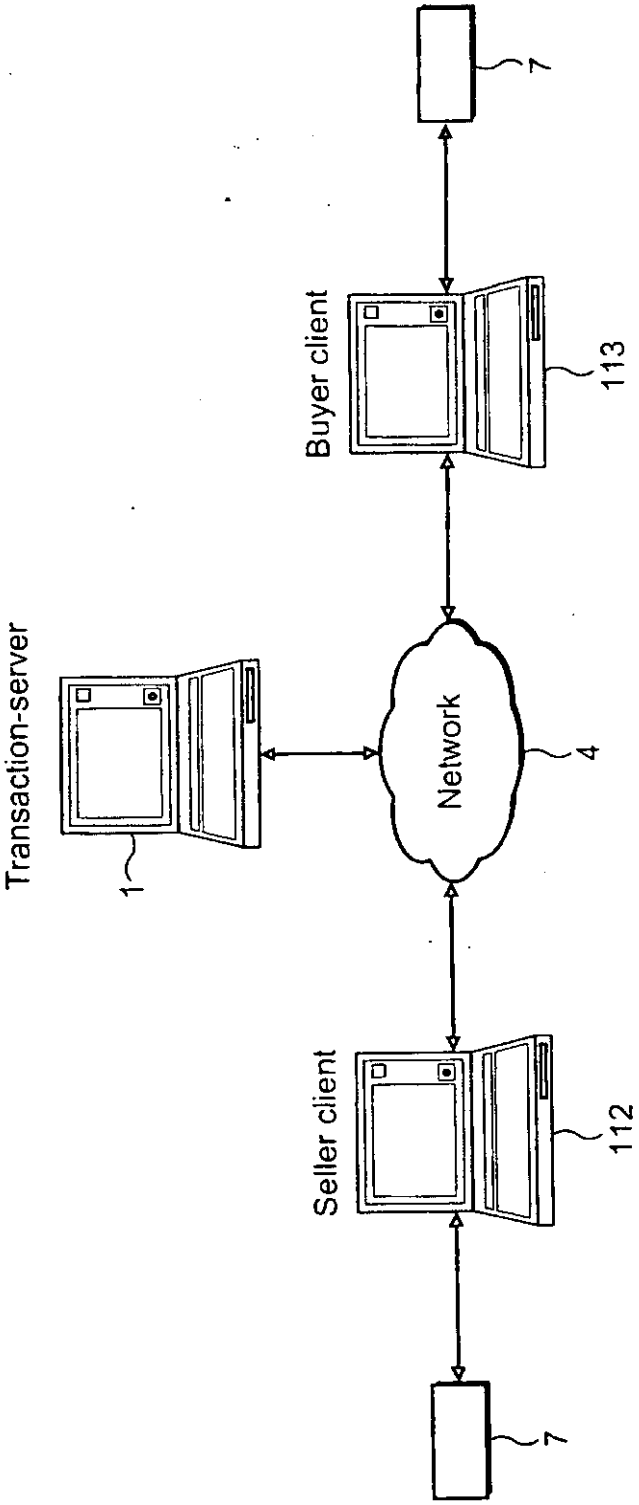

Transaction-server
1
Network
4
Buyer client
113
Seller client
112
7
· Obtain seller software
· Seller registers with transaction server using seller client processor
· Select client processor watermarks content
· Seller client processor informs transaction-server of the generated UMIDs and keys
· Seller provides metadata, rates card, business rules
· Seller sends watermarked material to buyer

FIG. 12



- Obtain buyer software
- Buyer registers with transaction server
- Buyer views watermarked content and decides to purchase
- Transmission server delivers license file
- Buyer client processor obtains removal data from license file
- Buyer client proceesor removes watermark and optionally adds fingerprint

FIG. 13

A

UMID(s)

Metadata

Link to seller
keywords
Picture stamp(s)
Resolution
Any other metadata

B

UMID(s)

Rates card

Price for additional metadata
Base price
Discounts
Exclusive purchase
Prices for different uses

C

UMID(s)

Business rules

Standard contract
Customized contract terms

D

UMID(s)

License file

a) Metadata
b) Purchase price
c) Business rules
d) Watermark data
e) Security data
f) Time limits
g) Country

FIG. 14

Statistics / Transaction log

Seller
Buyer
Content
Price
Total Sales
Total Price
Analysis by genre
Time expired material
Country / region analysis

FIG. 15

This Page Blank (uspto)